Universidade de Aveiro
Mestrado Integrado em Engenharia de Computadores e Telemática

1º Teste Teórico de Arquitetura de Redes
3 de Abril de 2013

Duração: 1h45m. Sem consulta. Justifique cuidadosamente todas as respostas.

1. Considerando o modelo de desenho hierárquico de redes e a rede em anexo onde as ligações entre os *swicthes* dos edifícios e os *switches* do núcleo (SWL3 C1 e SWL3 C2) são feitas usando ligações L2 multi-ponto, VLAN A e a VLAN B respetivamente. Admita ainda que: existem 3 VLAN distintas em cada edifício na camada de acesso da rede; cada VLAN nunca terá mais de 250 terminais; apenas uma VLAN (por edifício) necessita de 3 endereços IPv4 públicos; a rede DMZ precisa de 10 endereços IPv4 públicos; possui a gama de endereços privados IPv4 10.100.0.0/16, a gama de endereços públicos IPv4 193.1.1.0/26 e a gama de endereços IPv6 2001:F:F::/60.
   a) Defina e atribua as sub-redes IPv4 e IPv6 necessárias (para toda a rede e seus mecanismos). (2.0 valores)
   b) Descreva o que necessita instalar/configurar para que os endereços IPv4 possam ser atribuídos de forma dinâmica em toda a rede. (1.0 valores)
   c) Descreva como os terminais IPv6 irão obter os endereços *link-local* e global em modo de auto-configuração *stateless*. (1.0 valores)

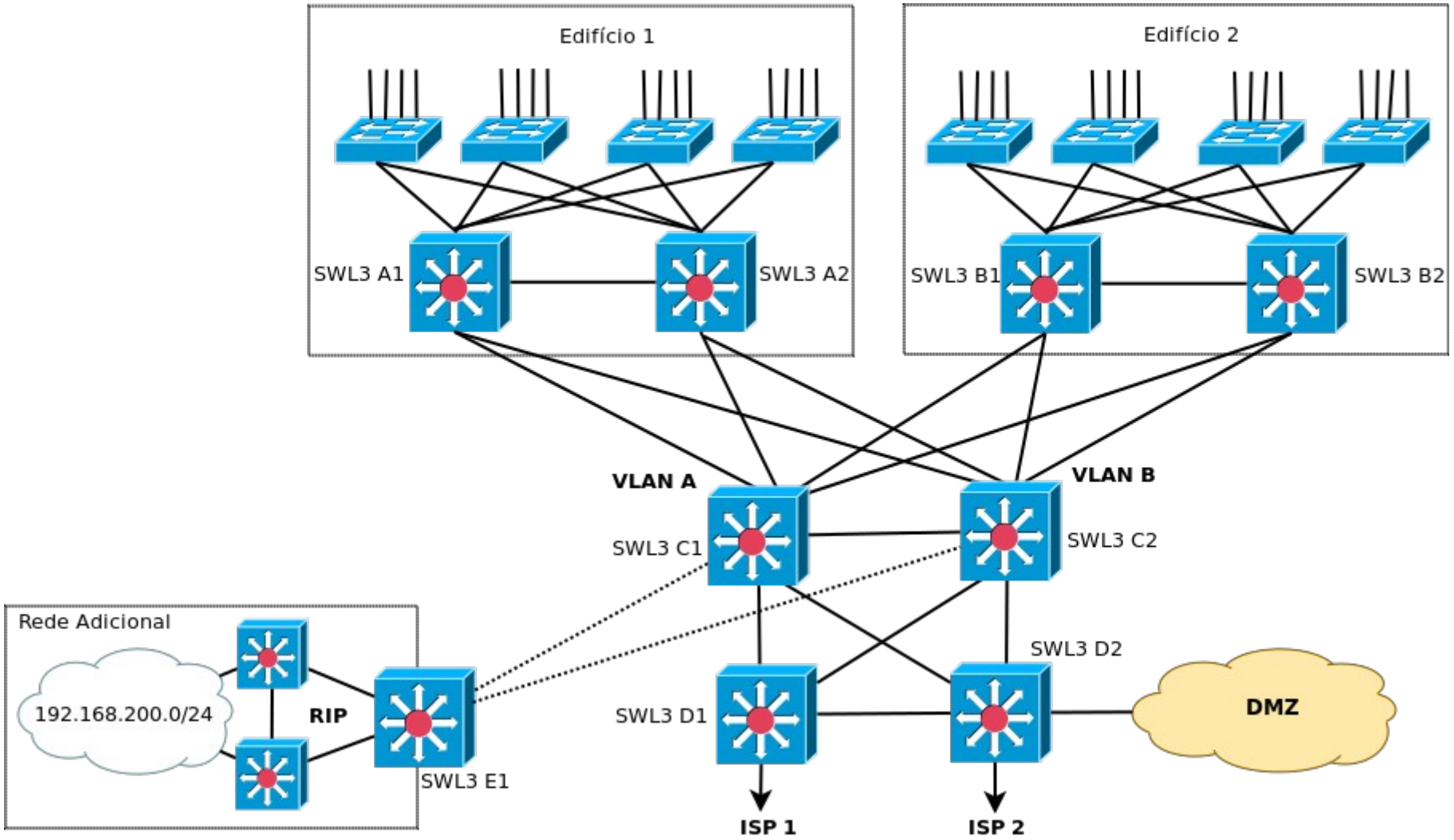
2. a) Considerando a rede em anexo (sem a "Rede Adicional"), indique que mecanismos necessita configurar nos *switches* fronteira (SWL3 D1 e D2) de modo a que todos os terminais internos com endereçamento privado IPv4 tenham conectividade com a Internet. Assuma a possibilidade de existir encaminhamento assimétrico entre os ISP1 e ISP2. Justifique. (1.5 valores)
   b) Considerando agora que a rede "Rede Adicional" foi interligada à rede principal, é necessário alterar/adicional alguma configuração nos *switches* fronteira (SWL3 D1 e D2) de modo a que todos os terminais internos da "Rede Adicional" tenham conectividade com a Internet? Se sim, quais? Justifique. (1.0 valores)

3. Admitindo que todos os *switches Layer3* têm os protocolos OSPFv2 e OSPFv3 ativos, que todos os interfaces têm um custo OSPF por omissão de 1, que os *switches* de acesso à Internet estão a anunciar (por OSPF) uma rota por omissão com uma métrica base de 10 (do tipo 1). Considere inicialmente que as redes da "Rede Adicional" estão a ser redistribuídas (com métrica do tipo 2) para o processo de OSPFv2 da rede principal.
   a) Escreva as tabelas de encaminhamento IPv4 e IPv6 do SWL3 E1. Nota: Considere as sub-redes definidas na questão 2. Caso não tenha respondido à questão 1a), identifique a rede IP por um identificador alfanumérico explícito (ex: redeIPV4vlan1.edificio1) (3.5 valores)
   b) Caso os processos de OSPF sejam parados no SWL3 D1 haverá alteração na tabela de encaminhamento do SWL3 A1? Se sim qual? Justifique. (1.5 valores)
   c) Caso a redistribuição de rotas no SWL3 E1 passe a ser to tipo 1, haverá alteração na tabela de encaminhamento do SWL3 A1? Se sim qual? Justifique. (1.5 valores)
   d) Nas redes dos edifícios, que configurações deverão ser feitas de modo a garantir que o tráfego para redes não pertencentes ao edifício nunca seja enviado para os *switches* L2 da camada de acesso? Justifique. (1.0 valores)
   e) Indique quais as configurações do OSPF a efetuar de modo a que: (i) o tráfego da Internet para uma VLAN específica do edifício 1 (ex: VLAN1) seja encaminhado preferencialmente pelo *switch* SWL3 A1, (ii) o restante tráfego da Internet para as outras VLAN seja encaminhado alternadamente pelo *switches* SWL3 A1 e A2 e (iii) a ligação entre os *switches* SWL3 A1 e A2 seja só usada em último recurso. (1.5 valores)

(continua)►

4. Assumindo que a rede possui servidores de DNS próprios instalados na rede, que na rede DMZ tem servidores que fornecem serviços ao exterior e e internamente tem servidores que apenas fornecem serviços aos terminais internos.
   a) Indique a localização ideal dos servidores para prestação de serviços internos. (1.0 valores)
   b) Indique a localização e conteúdo genérico (não necessita de referir os registos específicos) dos servidores DNS. (1.0 valores)
   c) Indique os passos a seguir de modo a implementar DNSSEC nos servidores de DNS. (1.5 valores)

Nome:_____ Número:_____


Edifício 1
Edifício 2
SWL3 A1
SWL3 A2
SWL3 B1
SWL3 B2
VLAN A
VLAN B
SWL3 C1
SWL3 C2
Rede Adicional
192.168.200.0/24
RIP
SWL3 E1
SWL3 D1
SWL3 D2
DMZ
ISP 1
ISP 2

Resolução

1a)
Endereços IPv4 privados
VLANx do edifício y → 10.100.2xy.0/24
VLAN A → 10.100.100.0/24
VLAN B → 10.100.101.0/24
Rede A1-A2 → 10.100.1.0/24 ou 10.100.1.0/30
Rede B1-B2 → 10.100.2.0/24 ou 10.100.1.4/30
Rede C1-C2 → 10.100.3.0/24 ou 10.100.1.8/30
Rede C1-D1 → 10.100.4.0/24 ou 10.100.1.12/30
Rede C1-D2 → 10.100.5.0/24 ou 10.100.1.16/30
Rede C2-D1 → 10.100.6.0/24 ou 10.100.1.20/30
Rede C2-D2 → 10.100.7.0/24 ou 10.100.1.24/30
Rede D1-D2 → 10.100.8.0/24 ou 10.100.1.28/30
DMZ → 10.100.10.0/24
(opcional) Rede E1-C1 → 10.100.11.0/24
(opcional) Rede E1-C2 → 10.100.12.0/24

Endereços IPv4 públicos
A rede 193.1.1.0/26 apenas contem os endereços de 193.1.1.0 a 193.1.1.64.

VLANx do edifício 1 (3 terminais+2 gateways+ID+Broadcast = 7→8→bloco /29) → 193.1.1.0/29
VLANx do edifício 2 (3 terminais+2 gateways+ID+Broadcast = 7→8→bloco /29) → 193.1.1.8/29
DMZ (10 terminais+1 gateway+ID+Broadcast = 13 → 16 → bloco /28) → 193.1.1.16/28
Para o NAT (os restantes → bloco /27) → 193.1.1.32/27
Outra solução possível: 193.1.1.0/28, 193.1.1.16/28, 193.1.1.32/28, 193.1.1.48/28.

Endereços IPv6 globais
A máscara /60 apenas deixa disponíveis 16 subnets com máscara /64 (2^(64-60)) → 0000 até 000F
VLAN1 do edifício 1 → 2001:F:F:0000::/64
VLAN2 do edifício 1 → 2001:F:F:0001::/64
VLAN3 do edifício 1 → 2001:F:F:0002::/64
VLAN1 do edifício 2 → 2001:F:F:0004::/64
VLAN2 do edifício 2 → 2001:F:F:0005::/64
VLAN3 do edifício 2 → 2001:F:F:0006::/64
DMZ → 2001:F:F:000A::/64

As redes de interligação como vão usar endereços IPv6 permanentes e não possuem terminais podem pertencer a redes IPv6 com máscara maior que /64 (no limite /126 – para restarem 2 bits para diferenciar ambos os routers/switches). Assim, uma solução possível é:
Rede A1-A2 → 2001:F:F:000F::10/126
Rede B1-B2 → 2001:F:F:000F::20/126
Rede C1-C2 → 2001:F:F:000F::30/126
Rede C1-D1 → 2001:F:F:000F::40/126
Rede C1-D2 → 2001:F:F:000F::50/126
Rede C2-D1 → 2001:F:F:000F::60/126
Rede C2-D2 → 2001:F:F:000F::70/126
Rede D1-D2 → 2001:F:F:000F::80/126
Rede D1-D2 → 2001:F:F:000F::90/126
(opcional) Rede E1-C1 → 2001:F:F:000F::B0/126
(opcional) Rede E1-C2 → 2001:F:F:000F::C0/126

PS: O uso de /127 é possível mas desaconselhado. Ver: http://packetlife.net/blog/2010/may/6/ipv6-127-prefixes/
PS2: Se os routers/switches das redes de interligação não necessitarem de gestão remota via IPv6 (pouco provável/aconselhável para futuro) poderiam ficar apenas com endereços link-local nos interfaces das redes de interligação.
PS3: É possível que os routers/swicthes fiquem apenas com endereços link-local nos interfaces das redes de interligação, desde que se adicione um interface loopback com uma rede IPv6 global com máscara /128 para que seja este o IPv6 de contacto para gestão remota. Assim:

Loopback SWL3 Zx → 2001:F:F:000F::Zx/128

1b)
(i) É necessário instalar e configurar um (ou mais) servidores DHCP. O(s) servidor(es) deverão ser colocados em zona(s) central(centrais) da rede (ou nas camadas de distribuição ou no core). Os servidores deverão ter gamas de endereços atribuíveis por (V)LAN. Das gamas configuradas deverão ser excluídos os endereços IP configurados manualmente nos routers/switches/servidores.
(ii) Em todos os interfaces de routers/switches onde potencialmente existam terminais deverá ser configurado o mecanismo de "BOOTP Relay Agent" que reenvia os pacotes de DHCP para um servidor DHCP.

1c)
Os endereços IPv6 são constituídos por um prefixo de rede e um interface ID. Nos endereços Link-Local o prefixo de rede é pré-definido (FE80/10) e nos endereços globais (quando em auto-configuração stateless) é recebido nos pacotes "Router Advertisement" (RA) enviados pelos routers. O interface ID poderá ser construido pelo terminal de forma aleatória ou em função do seu endereço MAC de acordo com a norma EUI-64.
O endereço Link-Local é construido após a inicialização do terminal e o endereço global é obtido/construído após a receção de um pacote RA de um router IPv6.

2a)
É necessário configurar o mecanismo de NAT/PAT, definindo a gama de endereços privados a traduzir e a gama de endereços públicos utilizáveis para a tradução. Como existem dois routers de acesso à Internet e um pacote que saia por um pode entrar na rede por outro (routing assimétrico na Internet), é necessário configurar um mecanismo de sincronização das tabelas/estado da tradução NAT/PAT, usando por exemplo "Stateful NAT" (SNAT).

2b)
É necessário atualizar a configuração do NAT/PAT/SNAT de modo a que os endereços na nova rede privada (192.168.200.0/24) sejam igualmente traduzidos.

(Opcional) Caso existam troca de rotas com os ISP é preciso garantir que a nova rede privada não é anunciada.

3a)

Tabela encaminhamento IPv4

C (redes da Rede Adicional diretamente ligadas) diretamente ligada
R 192.168.200.0/24, custo 1, via IPsw_cima, int_cima
, custo 1, via IPsw_baixo, int_baixo
R (outras redes da Rede Adicional) custo x, next-hop y, interface z
--
C Rede_E1C1, diretamente ligada
C Rede_E1C2, diretamente ligada
O RedeVLANxEDy, custo 3, via ipC1, int_para_C1 x=1,2,3;y=1,2
, custo 3, via ipC2, int_para_C2
O RedeVLANA, custo2, via ipC1, int_para_C1
O RedeVLANB, custo2, via ipC2, int_para_C2
O RedeC1C2, custo 2 , via ipC1, int_para_C1
, custo2, via ipC2, int_para_C2
O RedeA1A2, custo 3 , via ipC1, int_para_C1
, custo3, via ipC2, int_para_C2
O RedeB1B2, custo 3 , via ipC1, int_para_C1
, custo3, via ipC2, int_para_C2
O RedeD1D2, custo 3 , via ipC1, int_para_C1
, custo3, via ipC2, int_para_C2
O RedeC1Dx, custo 2 , via ipC1, int_para_C1 x=1,2
O RedeC2Dx, custo 2 , via ipC2, int_para_C2 x=1,2
--
O E1 0.0.0.0/0, custo12, via ipC1, int_para_C1
, custo12, via ipC2, int_para_C2

Tabela encaminhamento IPv6

--
C Rede_E1C1, diretamente ligada
C Rede_E1C2, diretamente ligada
O RedeVLANxEDy, custo 3, via ipC1, int_para_C1 x=1,2,3;y=1,2
, custo 3, via ipC2, int_para_C2
O RedeVLANA, custo2, via ipC1, int_para_C1
O RedeVLANB, custo2, via ipC2, int_para_C2
O RedeC1C2, custo 2 , via ipC1, int_para_C1
, custo2, via ipC2, int_para_C2
O RedeA1A2, custo 3 , via ipC1, int_para_C1
, custo3, via ipC2, int_para_C2
O RedeB1B2, custo 3 , via ipC1, int_para_C1
, custo3, via ipC2, int_para_C2
O RedeD1D2, custo 3 , via ipC1, int_para_C1
, custo3, via ipC2, int_para_C2
O RedeC1Dx, custo 2 , via ipC1, int_para_C1 x=1,2
O RedeC2Dx, custo 2 , via ipC2, int_para_C2 x=1,2
--
O E1 ::/0, custo12, via ipC1, int_para_C1
, custo12, via ipC2, int_para_C2

3b)

Não há qualquer alteração. O SWL3D1 não anuncia nenhuma rede em exclusivo, apenas deixa de anunciar uma rota por omissão. No entanto, os SWL3C1 e SWL3C2 escondem o facto de agora apenas haver uma rota por omissão a ser anunciada. O SWL3A1, continua a ver duas rotas por omissão via C1 e C2.

3c)
Sim, porque agora o custo das rotas da "Rede Adicional" passam a ser afetados pelo custo OSPF dos interfaces dos equipamentos que correm o protocolos OSPF. O custo de uma rota passará de x para x+2.

3d)
Os interfaces dos switches da camada de distribuição nos edifícios (A1, A2, B1 e B2) com as VLANs deverão ser configurados como "Interfaces Passivos". Assim nenhuma rede (externa ao edifício) será anunciada para as VLAN e consequentemente nenhuma rota será definida usando as VLAN.

Nota: A definição de áreas (sendo cada edifício uma área stub distinta) não garante que no caso extremo de um switch da distribuição de um edifício (por exemplo A1) perder todas as ligações ao *core* da rede não reencaminhe todo o tráfego pela área stub (VLANs) em direção ao core (área 0), visto que agora este switch apenas pertence à área stub.

3e)
A alteração deverá ser feita alterando os custos OSPF nos interfaces. Assim, (i) no interface VLAN1 do SWL3A2 o custo deverá ser aumentado (por exemplo para 2) de modo a ser superior ao custo do interface VLAN1 do SWL3A1 (o preferido para encaminhar o tráfego). (ii) Para garantir que para as restantes VLAN o tráfego é encaminhado alternadamente não é preciso mudar nada, já existem dois caminhos com custos iguais. (iii) Para garantir que a ligação entre A1-A2 só é usada em último recurso basta aumentar o custo para um valor grande superior ao das interfaces VLANx dos SWL3 A1 e A2 (por exemplo 10).

4a)
A localização ideal deverá ser numa rede diretamente ligada aos equipamentos de core, de modo a minimizar o tempo médio de acesso para todos os terminais da rede.

4b)
A localização do servidor DNS privado deverá ser numa rede diretamente ligada aos equipamentos de core (ver 4a) e esta rede não deverá ser acessível do exterior. O DNS público deverá ser colocado numa rede com acesso público (mesmo que condicionado) o mais perto possível dos routers de acesso à Internet (por exemplo DMZ).
O servidor DNS público apenas deverá conter registos DNS dos equipamentos da rede que possuem serviços de acesso público. O servidor DNS privado terá o mesmo conteúdo do público e os registos DNS referentes aos servidores e terminais internos/privados.

4c)
Para cada servidor DNS:
1 – Criar dois pares de chaves públicas-privadas. Um para assinar os registos DNS (ZSK) e outro para assinar a chave de assinatura de registos (KSK).
2 – As chaves públicas de verão ser colocadas nos ficheiros das respetivas zonas (registos DNSKEY).
3 – As chaves privadas deverão ser usadas para criar os registos RRSIG (assinaturas de registos) para todos os registos DNS existentes.
4 – Deverão ser criados os registos DS e DLV (que permitiram validar as chaves criadas). Os registos DS deverão ser exportados para o servidor DNS pai e os registos DLV para um servidor central.
(opcional) 5 – Receber (incluir nos respetivos ficheiros da zona) os registos DS dos servidores DNS filhos (delegações).